数理解析研究所講究録
155巻 1972年 3-13

Hecke operators の計算について

上智大 理工 和田秀男

Hecke operators の具体的な働きを計算するには、多項式の因数分解と虚2次体の類数を計算しなければならないので、まずこの2点について述べよう。

§1. 因数分解

有理整数を係数とする多項式:

$$F(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \cdots + a_n, \quad a_i \in \mathbb{Z}$$

を因数分解するには、$F(x) = 0$ の根 $x_1, x_2, \cdots, x_n$ の中より、r 個 $(1 \leqq r \leqq \frac{n}{2})$ $x_{f_1}, x_{f_2}, \cdots, x_{f_r}$ を選び出し、

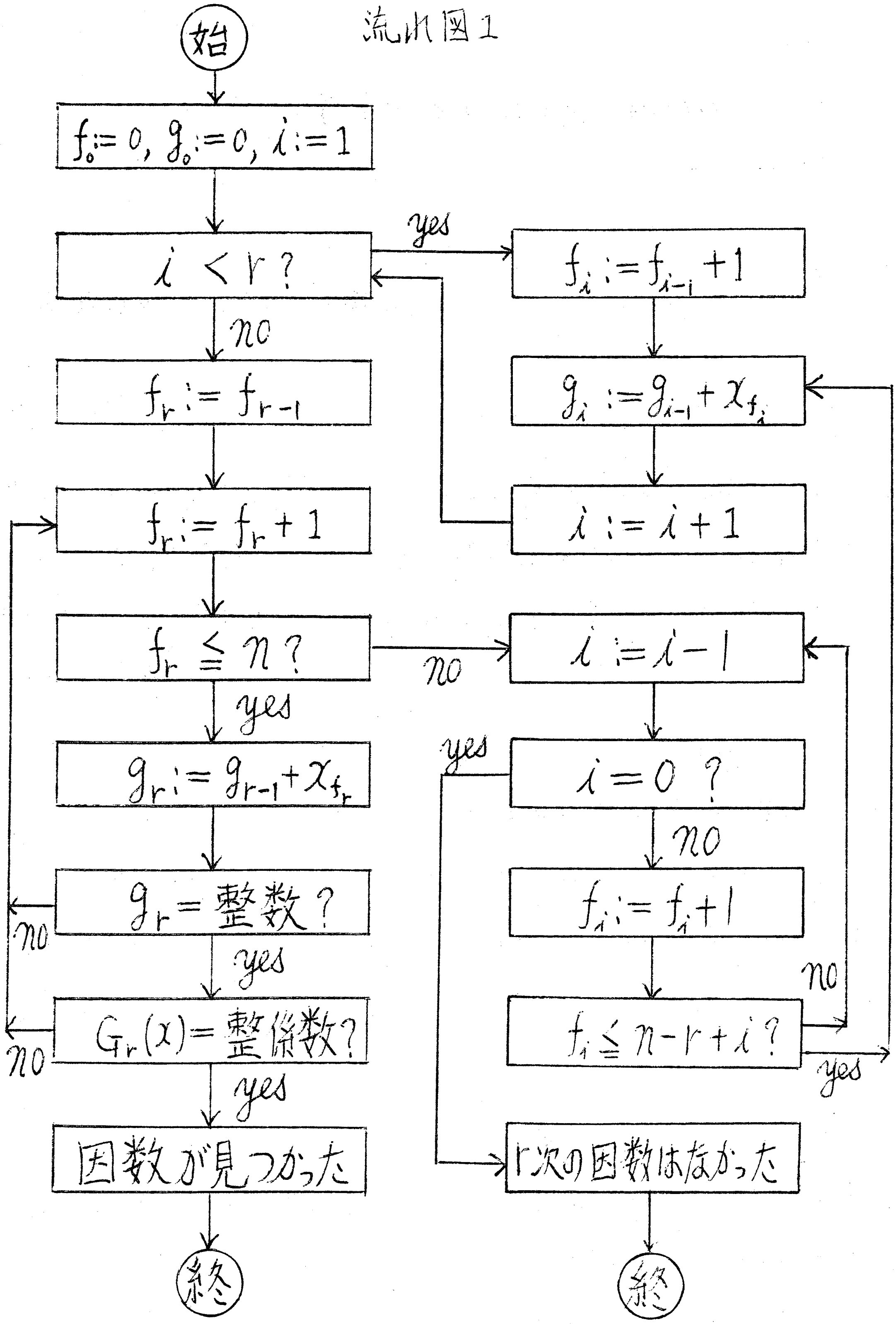
$$G_r(x) = (x - x_{f_1})(x - x_{f_2}) \cdots (x - x_{f_r})$$

が整係数になるかどうかをすべての組み合わせで調べれば良い。そのためにはまず

$$g_r = x_{f_1} + x_{f_2} + \cdots + x_{f_r}$$

4

流れ図1


始
$f_0 := 0,\ g_0 := 0,\ i := 1$
$i < r$?
yes
$f_i := f_{i-1} + 1$
$g_i := g_{i-1} + x_{f_i}$
$i := i + 1$
no
$f_r := f_{r-1}$
$f_r := f_r + 1$
$f_r \leqq n$?
no
$i := i - 1$
yes
$g_r := g_{r-1} + x_{f_r}$
yes
$i = 0$?
no
$g_r =$ 整数？
no
yes
$f_i := f_i + 1$
no
$G_r(x) =$ 整係数？
$f_i \leqq n - r + i$?
no
yes
yes
因数が見つかった
r次の因数はなかった
終
終

を計算し、g_rが整数のとき $G_r(x)$ を計算すれば良い。r個を選ぶすべての組み合わせを作る方法は流れ図1のようになる。実例として

$$F(x) = x^{18} + 79x^{17} + 2850x^{16} + 62285x^{15} + 922386x^{14}$$
$$+ 9809357x^{13} + 77456063x^{12} + 463047814x^{11}$$
$$+ 2117748840x^{10} + 7436199023x^{9} + 20000201335x^{8}$$
$$+ 40864981130x^{7} + 62492846639x^{6}$$
$$+ 69863925734x^{5} + 55066595198x^{4}$$
$$+ 28885227055x^{3} + 9115502993x^{2} + 1395936512x$$
$$+ 47367833$$

のとき、まず $F(x) = 0$ の根を計算してみると、すべて負根で近似値は

$$x_1 = -10.989395213965386179360830791621$$
$$x_2 = -10.372176552914877482949302815600$$
$$x_3 = -8.685121751541672674194381989894$$
$$x_4 = -7.790274736615651531405170850597$$
$$x_5 = -6.407976666889782759819381752687$$
$$x_6 = -6.180916186419658304393214101654$$
$$x_7 = -4.803782605994559553743521163324$$
$$x_8 = -4.329714748494450426992750972764$$
$$x_9 = -4.013314974138213865494777588338$$

$x_{10} = -\ 3.7607599183130828848591614165 99$

$x_{11} = -\ 3.0766334158079486482436263386 57$

$x_{12} = -\ 2.9129057478589086719000261274 93$

$x_{13} = -\ 1.6916861827407509119044746184 06$

$x_{14} = -\ 1.3553980500621128776087469363 55$

$x_{15} = -\ 1.3139089578700191779854265795 68$

$x_{16} = -\ 0.6982774647136882789247821881 67$

$x_{17} = -\ 0.5719447859469454103007400334 98$

$x_{18} = -\ 0.0458120397122903599193509119 41$

となった。この値をもとにして r 個（$1 \leqq r \leqq 9$）の根の和をすべての組み合わせで調べてみるとどれも整数にならなかった。整数か否かは、小数点以下 8 個 0 がつづくか、または 8 個 9 がつづくかで判定した。最後に根の近似値を使って用心深く $(x-x_1)(x-x_2)\cdots\cdots(x-x_{18})$ を計算してみると

$$= x^{18} + 78.99999999999999999999667177186\,x^{17}$$

$$+ 2849.999999999999999999997522218180\,x^{16}$$

$$+ 62284.999999999999999999163974924\,x^{15}$$

$$+ 922385.99999999999999998305786192\,x^{14}$$

$$+ 9809356.999999999999999769591 0104\,x^{13}$$

$$+ 77456062.99999999999999977435 3944\,x^{12}$$

$$
\begin{aligned}
&+463047813.99999999999998423619534\,x^{11}\\
&+2117748839.9999999999999166733150\,x^{10}\\
&+7436199022.9999999999996685876174\,x^{9}\\
&+20000201334.999999999999007498180\,x^{8}\\
&+40864981129.999999999997775447950\,x^{7}\\
&+62492846638.999999999996317573466\,x^{6}\\
&+69863925733.999999999995597032842\,x^{5}\\
&+55066595197.999999999996328720586\,x^{4}\\
&+28885227054.999999999979830037900\,x^{3}\\
&+9115502992.9999999999993395083560\,x^{2}\\
&+13959365511.999999999998960104250\,x\\
&+47367832.999999999999996443617034
\end{aligned}
$$

となった。よって整数か否かの判定を8個0または9がならぶか否かで調べたのは安全な方法であったことがわかる。つまり $F(x)$ は既約である。根を計算する時間を別にすれば、津田塾大学にある小型計算機 TOSBAC−3000 で35秒で、$F(x)$ が既約だと判定された。

§2、虚2次体の類数

自然数 d_0 を素数の2乗では割れない数とする。このとき

$$d = \begin{cases} d_0, & d_0 \equiv 3 \pmod 4 \text{ のとき} \\ 4d_0, & d_0 \not\equiv 3 \pmod 4 \text{ のとき} \end{cases}$$

と d を定める。$(-d)$ を判別式に持つ虚2次体の類数 $h = h(-d)$ とは

(1) $b^2 - 4ac = -d$

(2) $|b| \leqq a \leqq c$

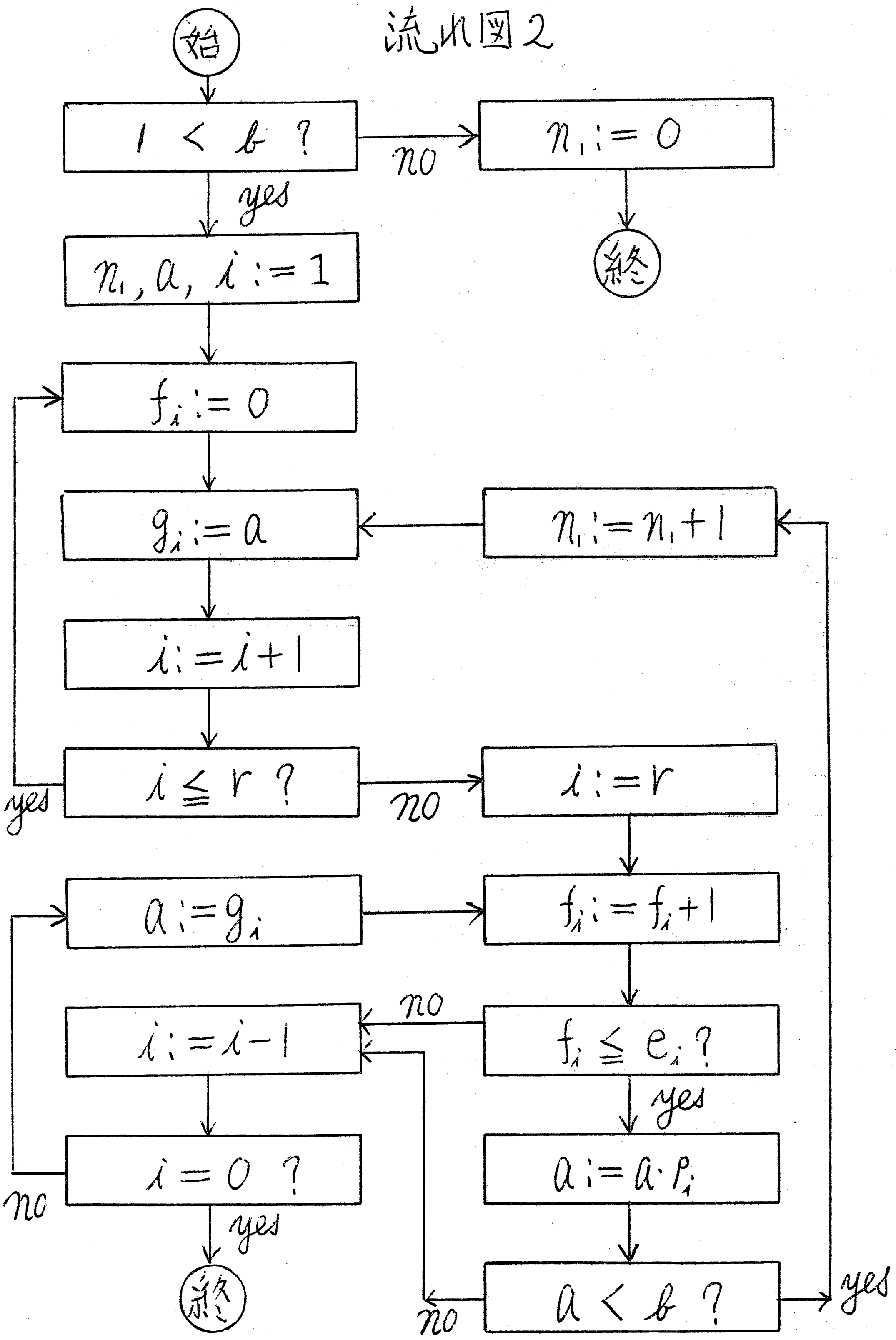
を満たす整数 a, b, c の組み合わせの個数である。ただし $|b| = a$ または $a = c$ が成り立つときは、b は正の値のみに限る。

さてこのとき $-d = b^2 - 4 \cdot a \cdot c \leqq b^2 - 4 \cdot b \cdot b = -3b^2$, したがって $b^2 \leqq d/3$ となる。$b\ (\geqq 0)$ を固定したとき、$y = (b^2 + d)/4$ とおくと、a, c は y の約数である。いかに能率的に a, c の組み合わせの個数を求めるか、考えてみよう。

(A) $b = 0$ のとき、y の約数の個数を n とすると $y = a \cdot c$, $a \leqq c$ となる組み合わせの個数は $[(n+1)/2]$ 通りである。

(B) $b \neq 0$ のとき、y の約数の個数を n, そのうち b より小さくなる個数を n_1 とすれば、($y = a \cdot c$, $b < a < c$ となる a, c の組み合わせ) $\times 2 +$ ($y = a \cdot c$, $b = a$ または $a = c$ となる a, c の組み合わせ) は

流れ図2


始
1 < b ?
no
$n_1 := 0$
終
yes
$n_1, a, i := 1$
$f_i := 0$
$g_i := a$
$n_1 := n_1 + 1$
$i := i + 1$
$i \leqq r$?
yes
no
$i := r$
$a := g_i$
$f_i := f_i + 1$
no
$i := i - 1$
$f_i \leqq e_i$?
yes
$i = 0$?
no
yes
$a := a \cdot p_i$
終
$a < b$?
no
yes

$b \nmid y$ または $b^2 = y = 1$ のとき $(n - 2n_1)$ 通り，

$b \mid y$，$b^2 < y$ のとき $(n - 2n_1 - 1)$ 通りとなる。

以上より、類数 $h(-d)$ を計算するには、y を

$$y = p_1^{e_1} p_2^{e_2} \cdots\cdots p_r^{e_r}, \quad p_i = \text{素数}$$

と素因子分解し、その約数の個数 $n = \prod_{i=1}^{r} (1 + e_i)$ を計算するプログラムがまず必要である。次に y の約数

$$a = p_1^{f_1} p_2^{f_2} \cdots\cdots p_r^{f_r}, \quad (0 \leqq f_i \leqq e_i)$$

の中に $a < b$ となる a の個数 n_1 を計算するプログラムが必要である。n_1 は流れ図2で計算される。この図において g_i は

$$g_i = p_1^{f_1} p_2^{f_2} \cdots\cdots p_i^{f_i}$$

のつもりである。

§3. Hecke operators の計算

Hecke operator $T(m)$ とはあるベクトル空間 $V(q)$ より $V(q)$ への線型写像である。しかも $V(q)$ の base を適当に（m には無関係に）選ぶと

$$T(m) = \begin{pmatrix} x_1 & & & 0 \\ & x_2 & & \\ & & \ddots & \\ 0 & & & x_n \end{pmatrix}$$

と表わされることが、知られている。$x_1, x_2, \cdots, x_n$ を

求めることが目的だけれど、Eichler の公式により

$$\mathrm{tr}\,T(m)=x_1+x_2+\cdots+x_n=\sum_{s^2-4m<0}A(s,m)\cdot h(s^2-4m)+B(m)$$

と表わされることが知られている。$A(s,m)$，$B(m)$ は容易に計算出来る s，m の関数である．よって類数 $h(s^2-4m)$ が求まれば $\mathrm{tr}\,T(m)=x_1+x_2+\cdots+x_n$ は計算出来る。次に志村公式

$$T(p)^k=\sum_{0\leq r\leq \frac{k}{2}}\left\{\binom{k}{r}-\binom{k}{r-1}\right\}\cdot p^r\cdot T\left(p^{k-2r}\right),\ \left(p=\text{素数},\binom{n}{-1}=0\right)$$

を用いれば $\mathrm{tr}\,T(p)$，$\cdots$，$\mathrm{tr}\,T(p^n)$ より $\mathrm{tr}\,T(p)^2$，$\cdots$，$\mathrm{tr}\,T(p)^n$ が計算出来る．つまり

$$T(p)=\begin{pmatrix} x_1 & & & 0 \\ & x_2 & & \\ & & \ddots & \\ 0 & & & x_n \end{pmatrix}$$

としたとき、$x_1+x_2+\cdots+x_n$，$x_1^2+x_2^2+\cdots+x_n^2$，$\cdots$，$x_1^n+x_2^n+\cdots+x_n^n$ が求まる。これより Newton 公式を用いれば、x_1，x_2，$\cdots$，x_n を根とする方程式が定まる．よって x_1，x_2，$\cdots$，x_n の近似値が計算出来る。またその方程式を因数分解することにより、$T(p)$ の作用の仕方がより明らかになる．一般の m に対しては

(1) $T(m_1\cdot m_2)=T(m_1)\cdot T(m_2)$，　$(m_1,m_2)=1$

(2) $T(p^k)=T(p)\cdot T(p^{k-1})-p\cdot T(p^{k-2})$，　$p=\text{素数}$

を用いれば良い。

ところでdが大きいと、$h(-d)$ を計算するのに時間がかかる。また、mが大きいと $s^2-4m<0$ となるsの個数も多くなる。例えば $q=239$ のとき $\dim V(q)=20$. よって $T(2)$ を求めるには、$\mathrm{tr}\,T(2)$, $\mathrm{tr}\,T(2^2)$, $\cdots$, $\mathrm{tr}\,T(2^{20})$ を計算しなければならない。$\mathrm{tr}\,T(2^{20})$ を計算するには、TOSBAC−3000 で約1時間かかる。$\mathrm{tr}\,T(m)$ を求める時間はmにほぼ比例するから、正直に $T(3)$ を求めるために $\mathrm{tr}\,T(3^{20})$ を計算すると400時間位かかってしまう。よって次のような工夫をする。まず

$$T(2^k)=\begin{pmatrix} a_1^{(k)} & & & 0 \\ & a_2^{(k)} & & \\ & & \ddots & \\ 0 & & & a_{20}^{(k)} \end{pmatrix},\qquad T(3)=\begin{pmatrix} y_1 & & & 0 \\ & y_2 & & \\ & & \ddots & \\ 0 & & & y_{20} \end{pmatrix}$$

とおく。$T(2)$ がわかれば $T(2^k)$ は(2)より計算出来る。次に(1)を用いれば

$$\begin{pmatrix} 1 & 1 & \cdots & 1 \\ a_1^{(1)} & a_2^{(1)} & \cdots & a_{20}^{(1)} \\ \vdots & & & \\ a_1^{(19)} & a_2^{(19)} & \cdots & a_{20}^{(19)} \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{20} \end{pmatrix}=\begin{pmatrix} \mathrm{tr}\,T(3) \\ \mathrm{tr}\,T(2\cdot 3) \\ \vdots \\ \mathrm{tr}\,T(2^{19}\cdot 3) \end{pmatrix}$$

となるので、この連立方程式を解けば $T(3)$ が求まる。同様に $T(5)$ を求めるには $\mathrm{tr}\,T(5)$, $\mathrm{tr}\,T(2\cdot 5)$, $\cdots$,

$\mathrm{tr}\,T(2^{10}\cdot 5)$, $\mathrm{tr}\,T(3\cdot 5)$, $\cdots$, $\mathrm{tr}\,T(3^{9}\cdot 5)$ を計算すれば良い。このように $T(1), T(2), T(3), \cdots, T(20)$ が求まれば、$T(p)$, $(p>20)$ は $\mathrm{tr}\,T(p)$, $\mathrm{tr}\,T(2p)$, $\mathrm{tr}\,T(3p)$, $\cdots$, $\mathrm{tr}\,T(20p)$ を計算すれば求まる。結局 $T(2), T(3)$ を求めるのに時間がかかり、他は桁違いに早く計算出来るわけである。